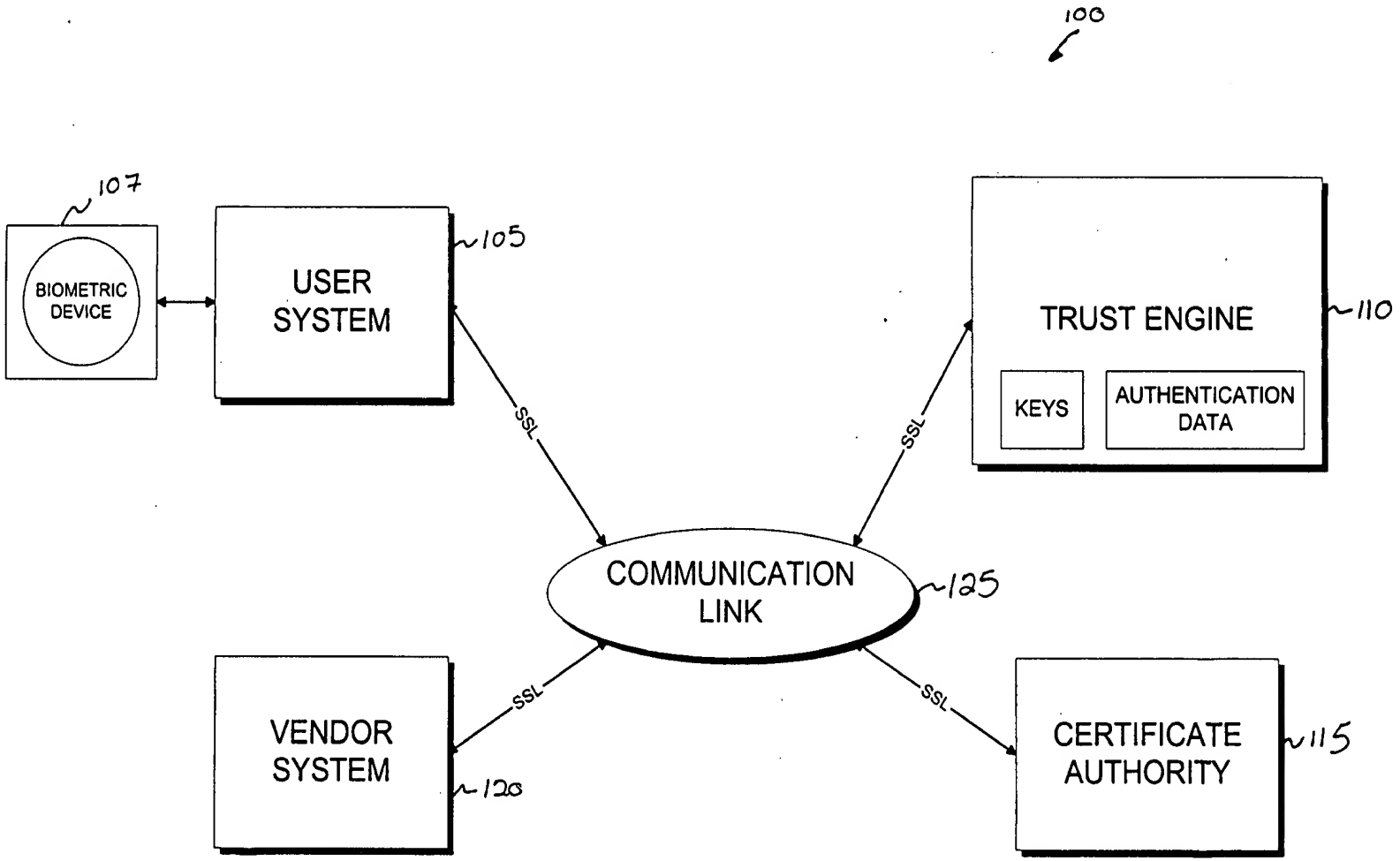


FIG. 1

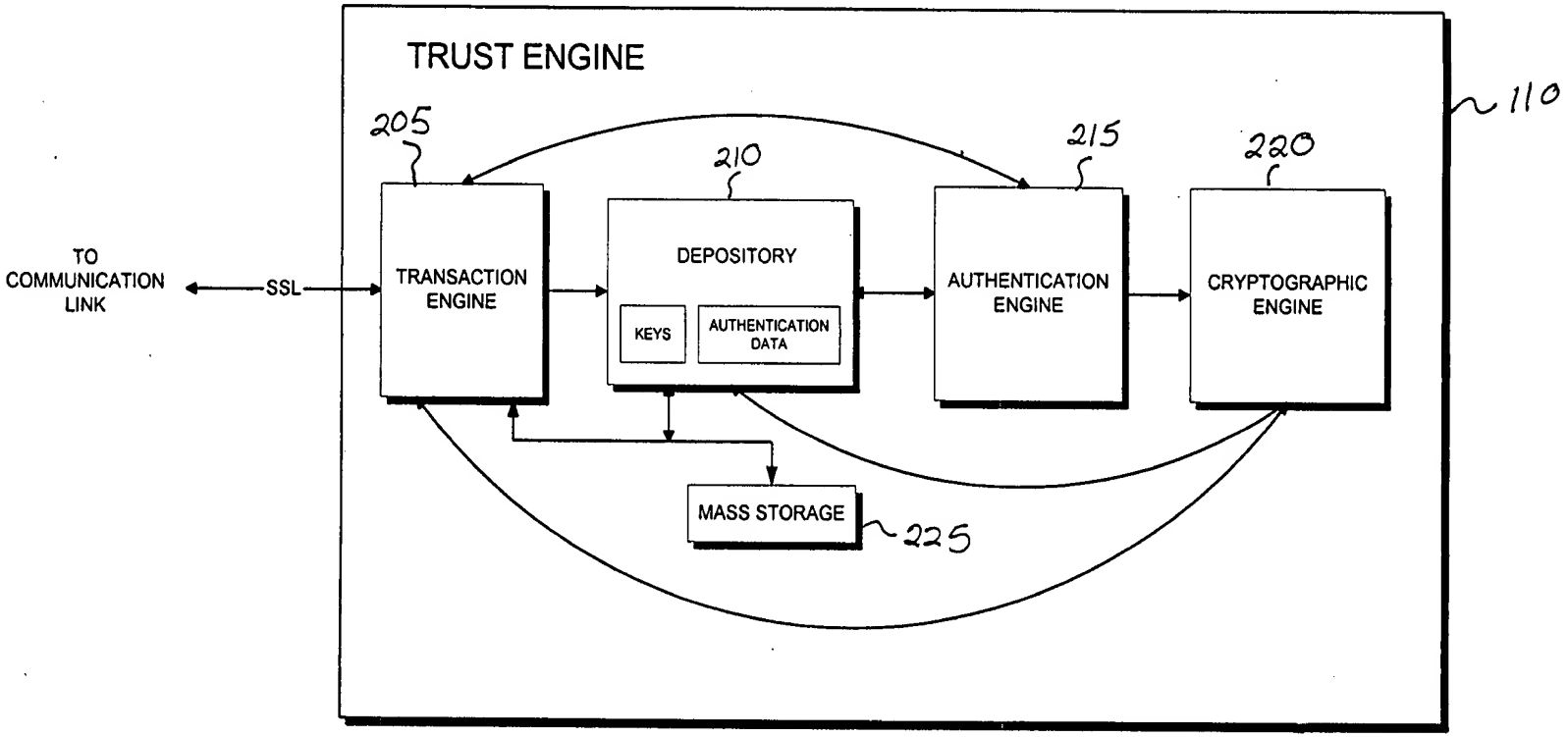

TRUST ENGINE
110
205
210
215
220
TO COMMUNICATION LINK
SSL
TRANSACTION ENGINE
DEPOSITORY
KEYS
AUTHENTICATION DATA
AUTHENTICATION ENGINE
CRYPTOGRAPHIC ENGINE
MASS STORAGE
225

FIG. 2

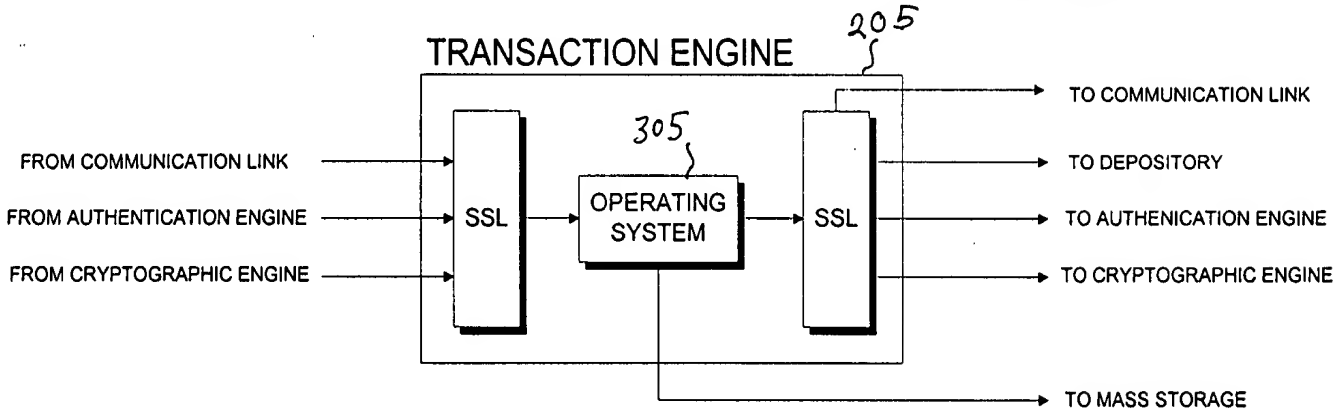

TRANSACTION ENGINE
205
305
FROM COMMUNICATION LINK
FROM AUTHENTICATION ENGINE
FROM CRYPTOGRAPHIC ENGINE
SSL
OPERATING SYSTEM
SSL
TO COMMUNICATION LINK
TO DEPOSITORY
TO AUTHENICATION ENGINE
TO CRYPTOGRAPHIC ENGINE
TO MASS STORAGE

FIG. 3

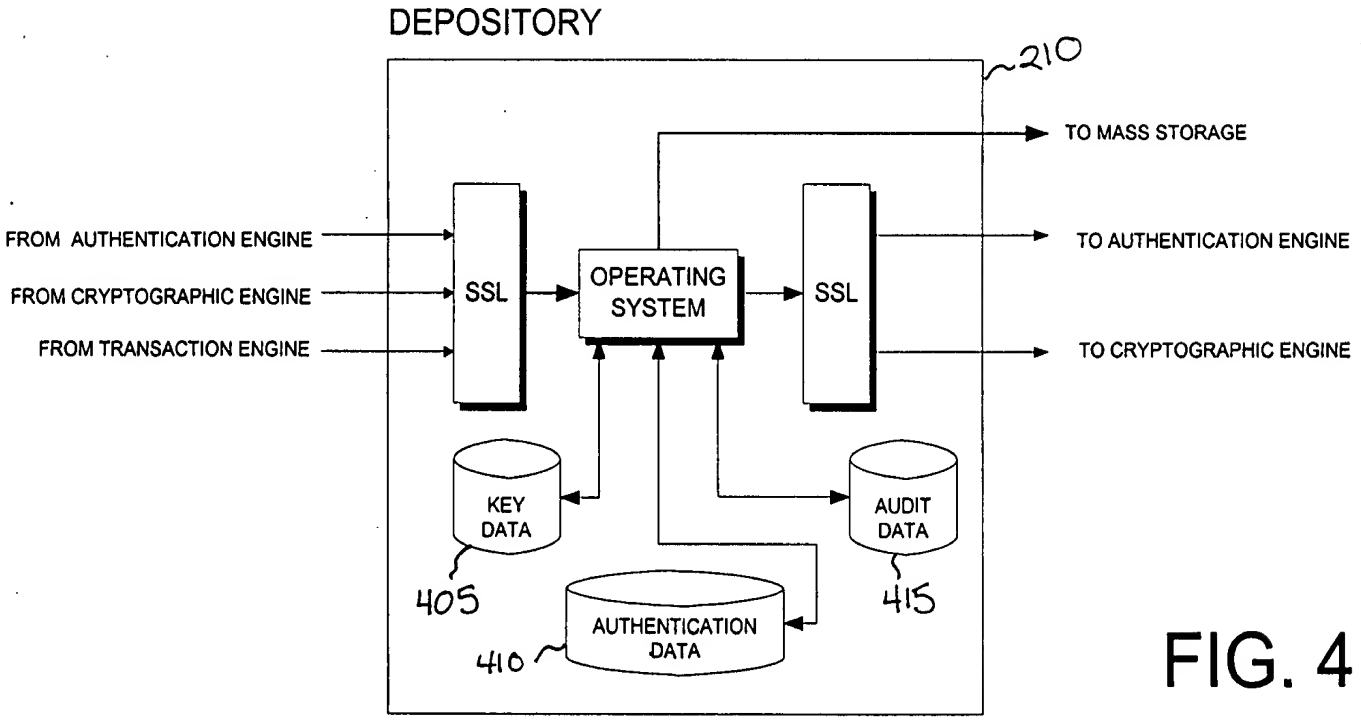

DEPOSITORY
210
FROM AUTHENTICATION ENGINE
FROM CRYPTOGRAPHIC ENGINE
FROM TRANSACTION ENGINE
SSL
OPERATING SYSTEM
SSL
TO MASS STORAGE
TO AUTHENTICATION ENGINE
TO CRYPTOGRAPHIC ENGINE
KEY DATA
405
AUDIT DATA
415
AUTHENTICATION DATA
410

FIG. 4

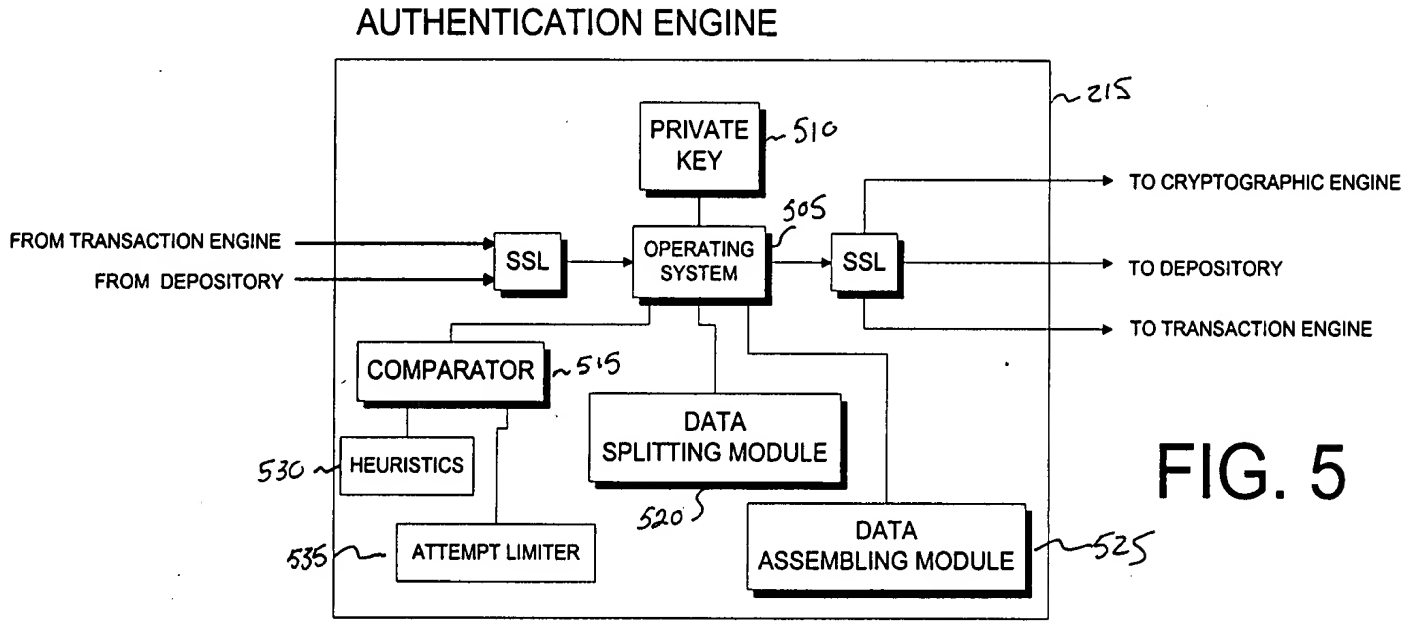

AUTHENTICATION ENGINE
215
PRIVATE KEY
510
505
FROM TRANSACTION ENGINE
FROM DEPOSITORY
SSL
OPERATING SYSTEM
SSL
TO CRYPTOGRAPHIC ENGINE
TO DEPOSITORY
TO TRANSACTION ENGINE
COMPARATOR
515
DATA SPLITTING MODULE
530
HEURISTICS
520
535
ATTEMPT LIMITER
DATA ASSEMBLING MODULE
525

FIG. 5

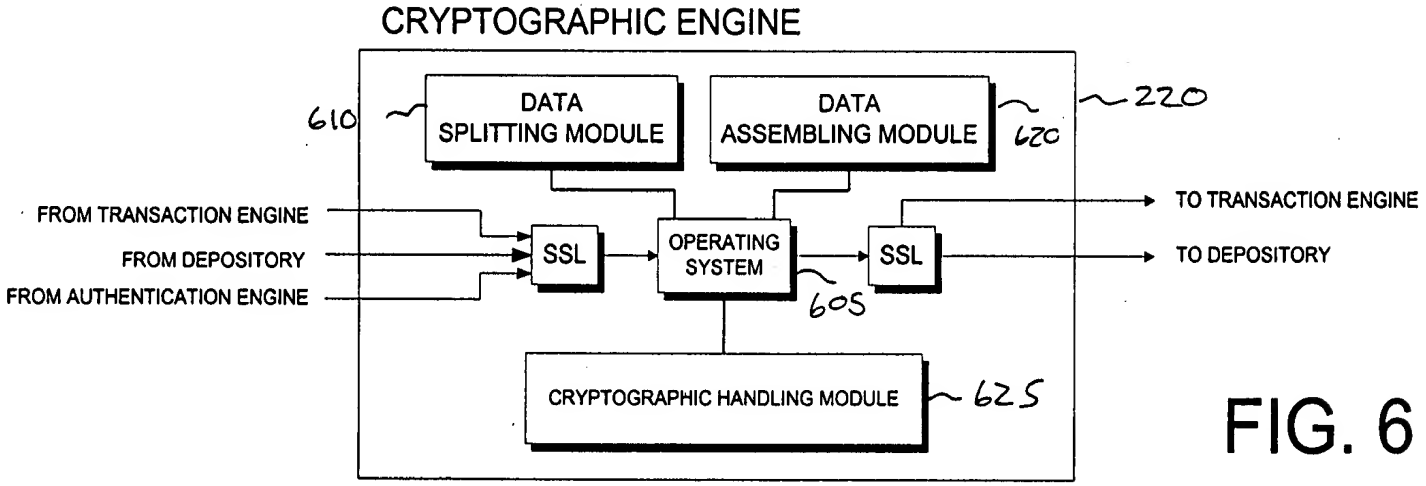

CRYPTOGRAPHIC ENGINE
610
DATA SPLITTING MODULE
DATA ASSEMBLING MODULE
620
220
FROM TRANSACTION ENGINE
FROM DEPOSITORY
FROM AUTHENTICATION ENGINE
SSL
OPERATING SYSTEM
605
SSL
TO TRANSACTION ENGINE
TO DEPOSITORY
CRYPTOGRAPHIC HANDLING MODULE
625

FIG. 6

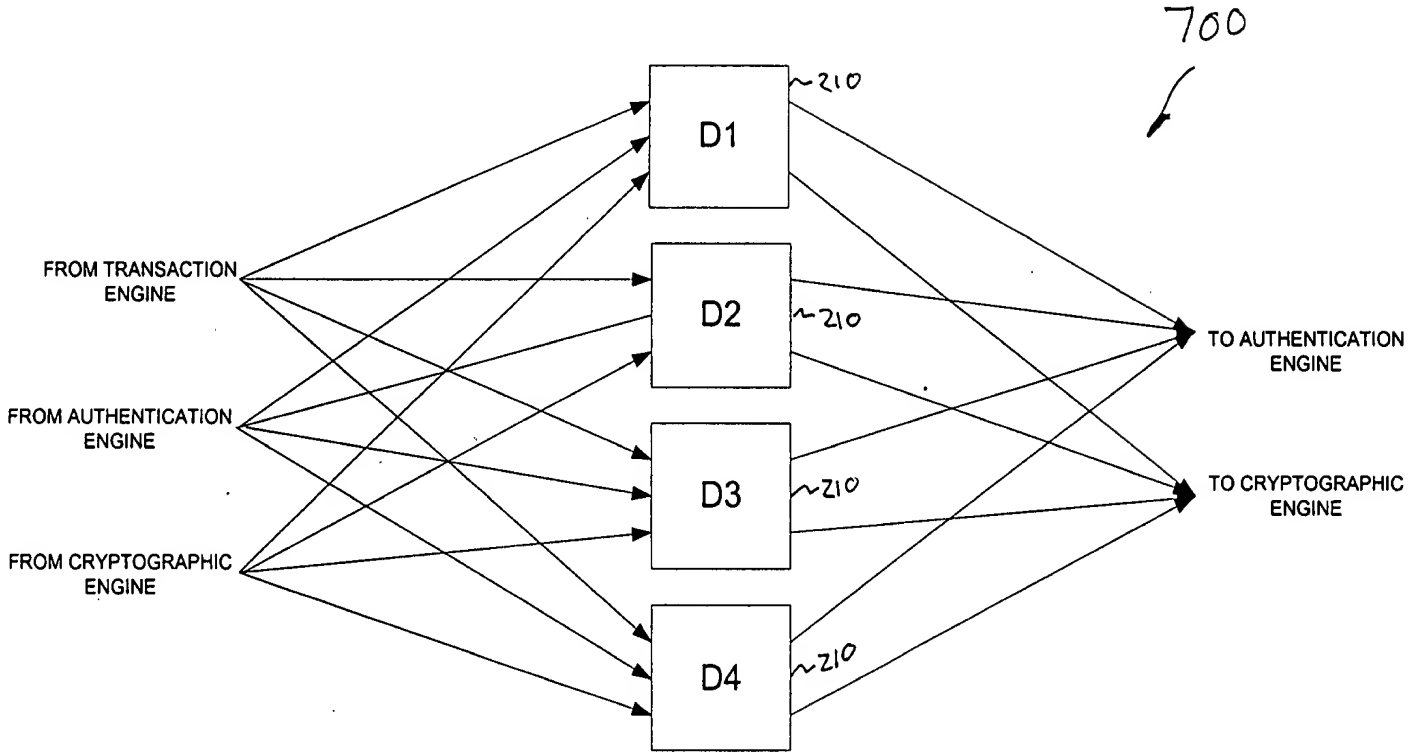

700
210
D1
D2
D3
D4
FROM TRANSACTION ENGINE
FROM AUTHENTICATION ENGINE
FROM CRYPTOGRAPHIC ENGINE
TO AUTHENTICATION ENGINE
TO CRYPTOGRAPHIC ENGINE

FIG. 7

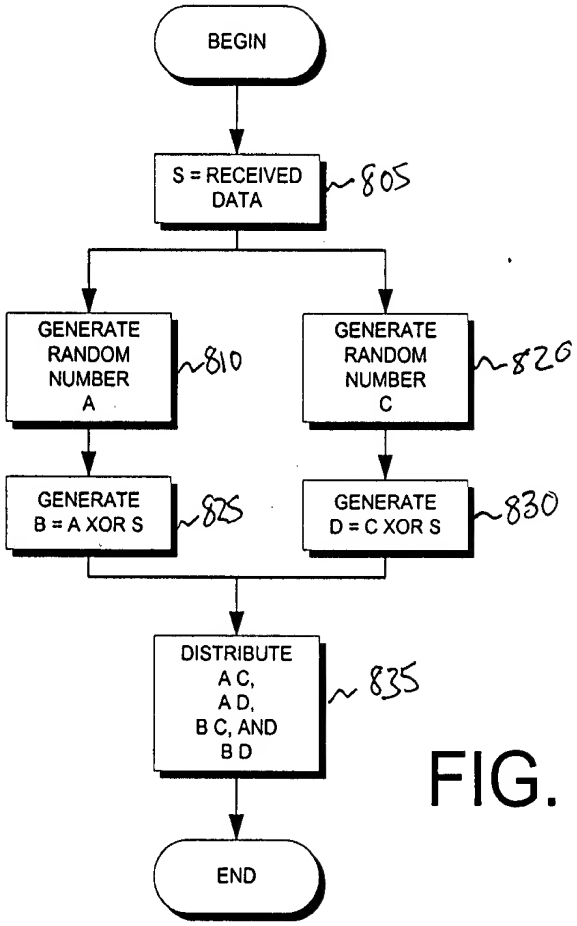

BEGIN
S = RECEIVED DATA
805
GENERATE RANDOM NUMBER A
810
GENERATE RANDOM NUMBER C
820
GENERATE B = A XOR S
825
GENERATE D = C XOR S
830
DISTRIBUTE A C, A D, B C, AND B D
835
END
800

FIG. 8

900

	ENROLLMENT DATA FLOW			
	SEND	**RECEIVE**	**SSL**	**ACTION**
905	USER	TRANSACTION ENGINE (TE)	½	TRANSMIT ENROLLMENT AUTHENTICATION DATA (B) AND THE USER ID (UID) ENCRYPTED WITH THE PUBLIC KEY OF THE AUTHENTICATION ENGINE (AE) AS (PUB_AE(UID, B))
915	TE	AE	FULL	FORWARD TRANSMISSION
920				AE DECRYPTS AND SPLITS FORWARDED DATA
925	AE	THE X^{TH} DEPOSITORY (DX)	FULL	STORE RESPECTIVE PORTION OF DATA
	WHEN DIGITAL CERTIFICATE REQUESTED			
930	AE	CRYPTOGRAPHIC ENGINE (CE)	FULL	REQUEST KEY GENERATION
935				CE GENERATES AND SPLITS KEY
945	CE	TE	FULL	TRANSMIT REQUEST FOR DIGITAL CERTIFICATE
950	TE	CERTIFICATION AUTHORITY (CA)	½	TRANSMIT REQUEST
955	CA	TE	½	TRANSMIT DIGITAL CERTIFICATE
960	TE	USER	½	TRANSMIT DIGITAL CERTIFICATE
	TE	MS	FULL	STORE DIGITAL CERTIFICATE
965	CE	DX	FULL	STORE RESPECTIVE PORTION OF KEY

FIG. 9A

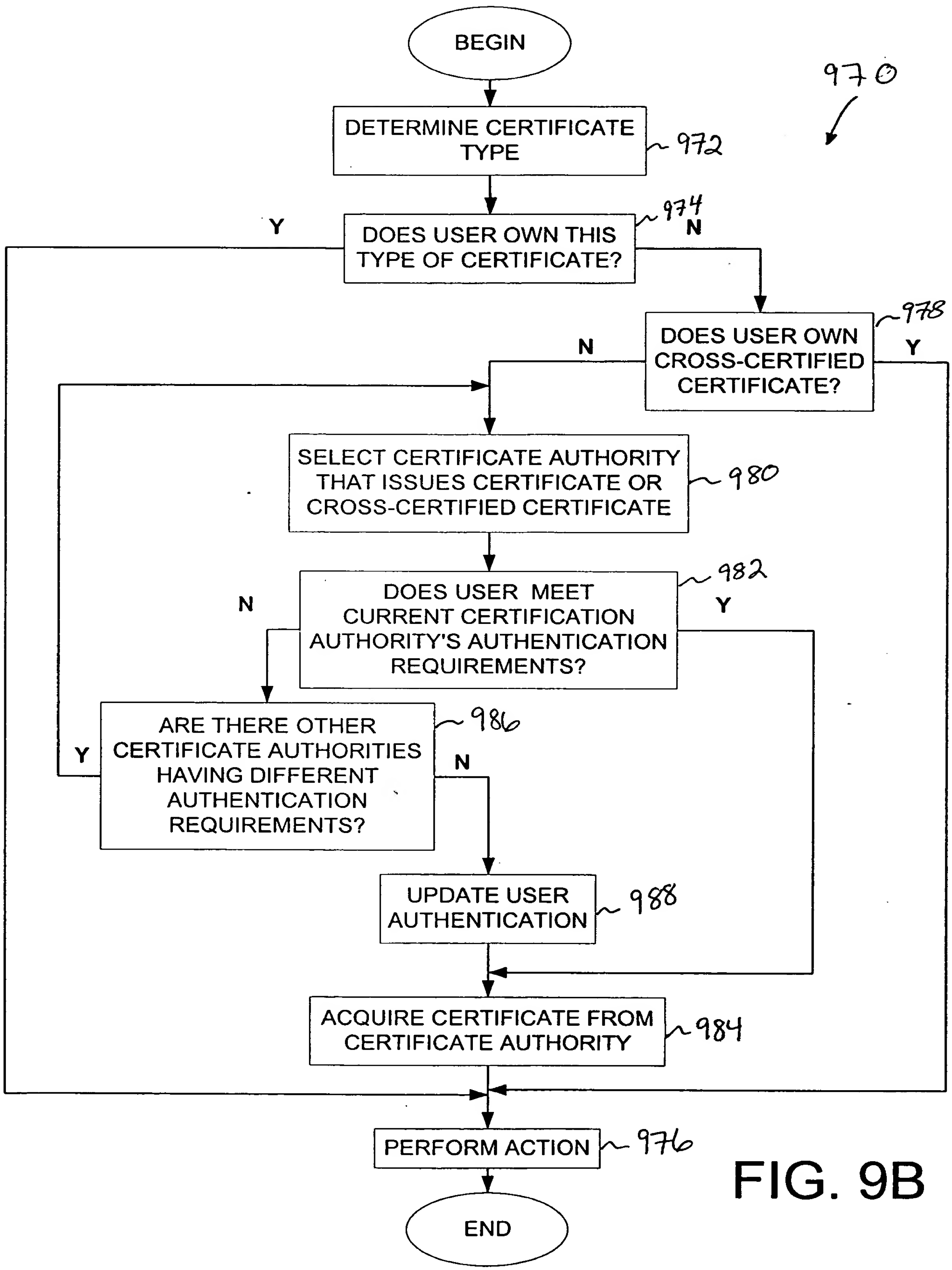


FIG. 9B

1000

	AUTHENTICATION DATA FLOW			
	SEND	**RECEIVE**	**SSL**	**ACTION**
1005	USER	VENDOR	½	TRANSACTION OCCURS, SUCH AS SELECTING PURCHASE
1010	VENDOR	USER	½	TRANSMIT TRANSACTION ID (TID), AND AUTHENTICATION REQUEST (AR)
				AUTHENTICATION DATA (B') IS GATHERED FROM USER
1015	USER	TE	½	TRANSMIT TID AND B' WRAPPED IN THE PUBLIC KEY OF THE AUTHENTICATION ENGINE (AE), AS (PUB_AE(TID, B'))
1020	TE	AE	FULL	FORWARD TRANSMISSION
				ENROLLMENT AUTHENTICATION DATA (B) IS REQUESTED AND GATHERED
1025	VENDOR	TRANSACTION ENGINE (TE)	FULL	TRANSMITS TID, AR
1030	TE	MASS STORAGE (MS)	FULL	CREATE RECORD IN DATABASE
1035	TE	THE X^{TH} DEPOSITORY (DX)	FULL	UID, TID
1040	DX	AE	FULL	TRANSMIT THE TID AND THE PORTION OF THE AUTHENTICATION DATA STORED AT ENROLLMENT (BX) AS (PUB_AE(TID, BX))
1045				AE ASSEMBLES B AND COMPARES TO B'
1050	AE	TE	FULL	TID, THE FILLED IN AR
1055	TE	VENDOR	FULL	TID, YES/NO
	TE	USER	½	TID, CONFIRMATION MESSAGE

FIG. 10

1100

SIGNING DATA FLOW			
SEND	**RECEIVE**	**SSL**	**ACTION**
USER	VENDOR	½	TRANSACTION OCCURS, SUCH AS AGREEING ON A DEAL
VENDOR	USER	½	TRANSMIT TRANSACTION IDENTIFICATION NUMBER (TID), AUTHENTICATION REQUEST (AR), AND AGREEMENT OR MESSAGE (M)
			CURRENT AUTHENTICATION DATA (B') AND A HASH OF THE MESSAGE RECEIVED BY THE USER (h(M')) IS GATHERED FROM USER
USER	TE	½	TRANSMIT TID, B', AR, AND h(M') WRAPPED IN THE PUBLIC KEY OF THE AUTHENTICATION ENGINE (AE) AS (PUB_AE(TID, B', h(M'))
TE	AE	FULL	FORWARD TRANSMISSION
			GATHER ENROLLMENT AUTHENTICATION DATA
VENDOR	TRANSACTION ENGINE (TE)	FULL	TRANSMITS UID, TID, AR, AND A HASH OF THE MESSAGE (h(M)).
TE	MASS STORAGE (MS)	FULL	CREATE RECORD IN DATABASE
TE	THE X^{TH} DEPOSITORY (DX)	FULL	UID, TID
DX	AE	FULL	TRANSMIT THE TID AND THE PORTION OF THE AUTHENTICATION DATA STORED AT ENROLLMENT (BX) AS (PUB_AE(TID, BX))
			THE ORIGINAL VENDOR MESSAGE IS TRANSMITTED TO THE AE
TE	AE	FULL	TRANSMIT h(M)
			AE ASSEMBLES B, COMPARES TO B' AND COMPARES h(M) TO h(M')
AE	CRYPTOGRAPHIC ENGINE (CE)	FULL	REQUEST FOR DIGITAL SIGNATURE AND A MESSAGE TO BE SIGNED, FOR EXAMPLE, THE HASHED MESSAGE
AE	DX	FULL	TID, SIGNING UID
DX	CE	FULL	TRANSMIT THE PORTION OF THE CRYPTOGRAPHIC KEY CORRESPONDING TO THE SIGNING PARTY
			CE ASSEMBLES KEY AND SIGNS
CE	AE	FULL	TRANSMIT THE DIGITAL SIGNATURE (S) OF SIGNING PARTY
AE	TE	FULL	TID, THE FILLED IN AR, h(M), AND S
TE	VENDOR	FULL	TID, A RECEIPT = (TID, YES/NO, AND S), AND THE DIGITAL SIGNATURE OF THE TRUSTENGINE, FOR EXAMPLE, A HASH OF THE RECEIPT ENCRYPTED WITH THE TRUSTENGINE'S PRIVATE KEY (Priv_TE(h(RECEIPT))
TE	USER	½	TID, CONFIRMATION MESSAGE

FIG. 11

1200

ENCRYPTION/DECRYPTION DATA FLOW			
SEND	**RECEIVE**	**SSL**	**ACTION**
DECRYPTION			
			PERFORM AUTHENTICATION DATA PROCESS 1000, INCLUDE THE SESSION KEY (SYNC) IN THE AR, WHERE THE SYNC HAS BEEN ENCRYPTED WITH THE PUBLIC KEY OF THE USER AS PUB_USER(SNYC)
			AUTHENTICATE THE USER
AE	CE	FULL	FORWARD PUB_USER(SYNC) TO CE
AE	DX	FULL	UID, TID
DX	CE	FULL	TRANSMIT THE TID AND THE PORTION OF THE PRIVATE KEY AS (PUB_AE(TID, KEY_USER))
			CE ASSEMBLES THE CRYPTOGRAPHIC KEY AND DECRYPTS THE SYNC
CE	AE	FULL	TID, THE FILLED IN AR INCLUDING DECRYPTED SYNC
AE	TE	FULL	FORWARD TO TE
TE	REQUESTING APP/VENDOR	½	TID, YES/NO, SYNC
ENCRYPTION			
REQUESTING APP/VENDOR	TE	½	REQUEST FOR PUBLIC KEY OF USER
TE	MS	FULL	REQUEST DIGITAL CERTIFICATE
MS	TE	FULL	TRANSMIT DIGITAL CERTIFICATE
TE	REQUESTING APP/VENDOR	½	TRANSMIT DIGITAL CERTIFICATE

1205
1210
1215
1220
1225
1230
1235
1240
1245
1250

FIG. 12

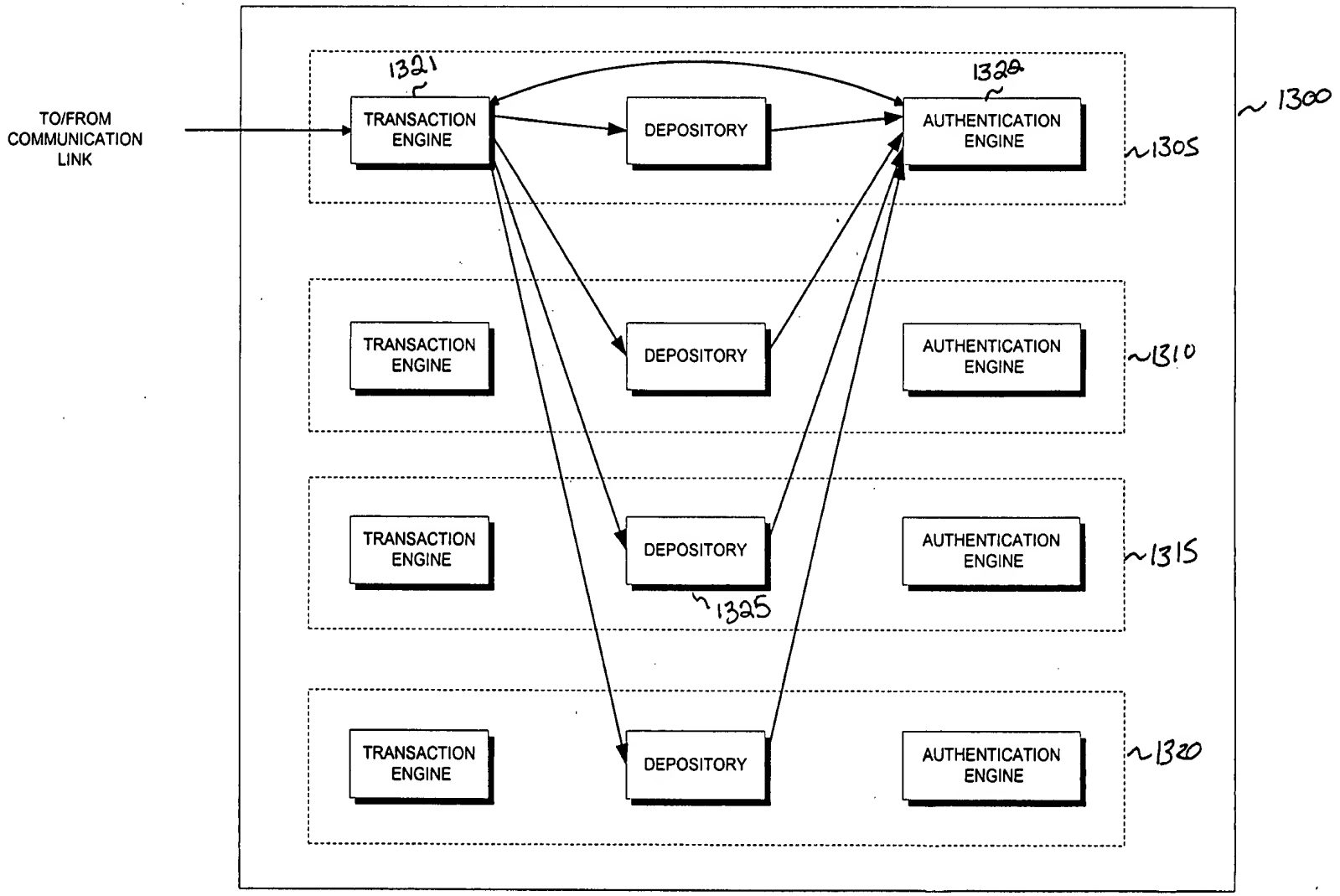


FIG. 13

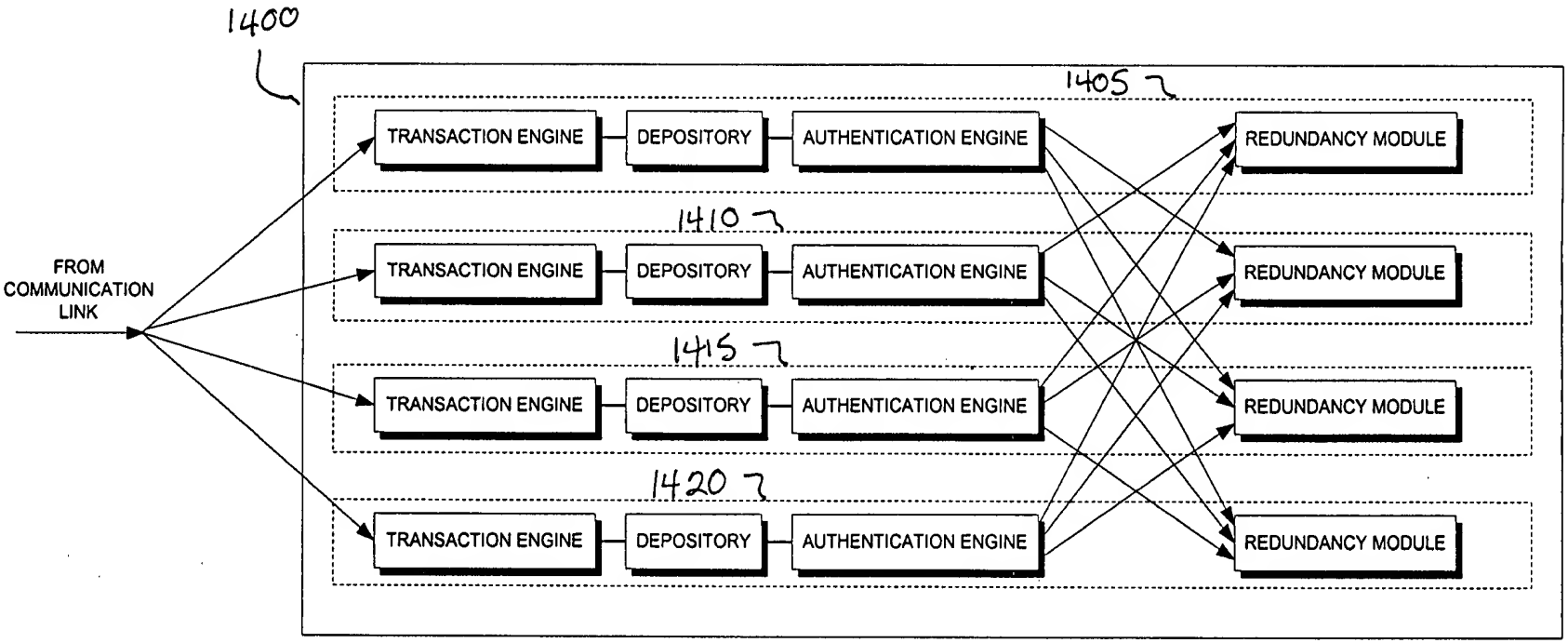


FIG. 14

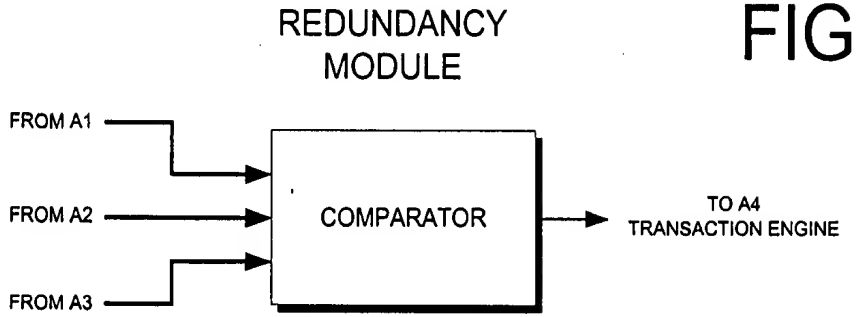
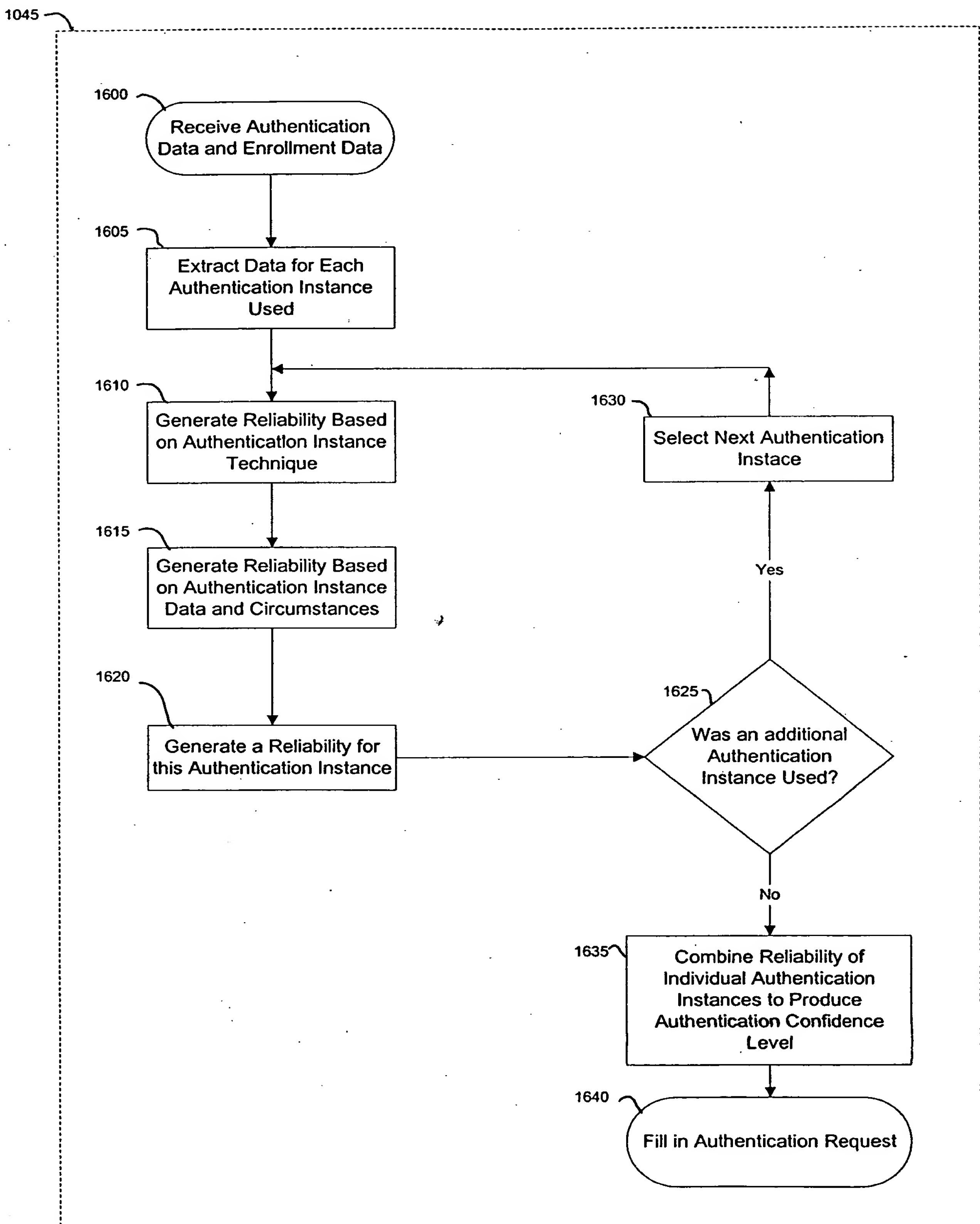


FIG. 15

FIGURE 16



1045
1600
Receive Authentication Data and Enrollment Data
1605
Extract Data for Each Authentication Instance Used
1610
Generate Reliability Based on Authentication Instance Technique
1615
Generate Reliability Based on Authentication Instance Data and Circumstances
1620
Generate a Reliability for this Authentication Instance
1625
Was an additional Authentication Instance Used?
Yes
1630
Select Next Authentication Instace
No
1635
Combine Reliability of Individual Authentication Instances to Produce Authentication Confidence Level
1640
Fill in Authentication Request

FIGURE 17

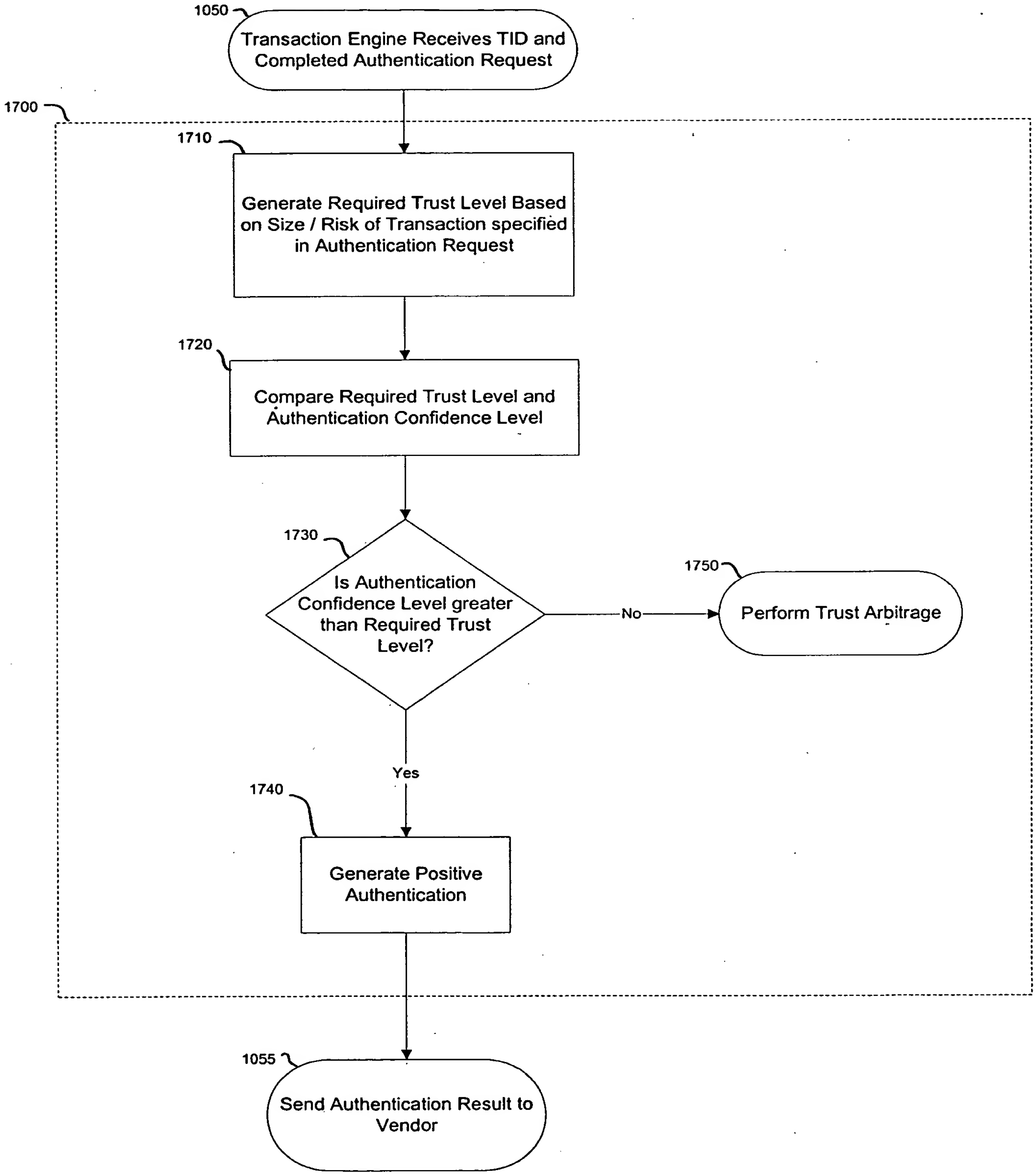


FIGURE 18

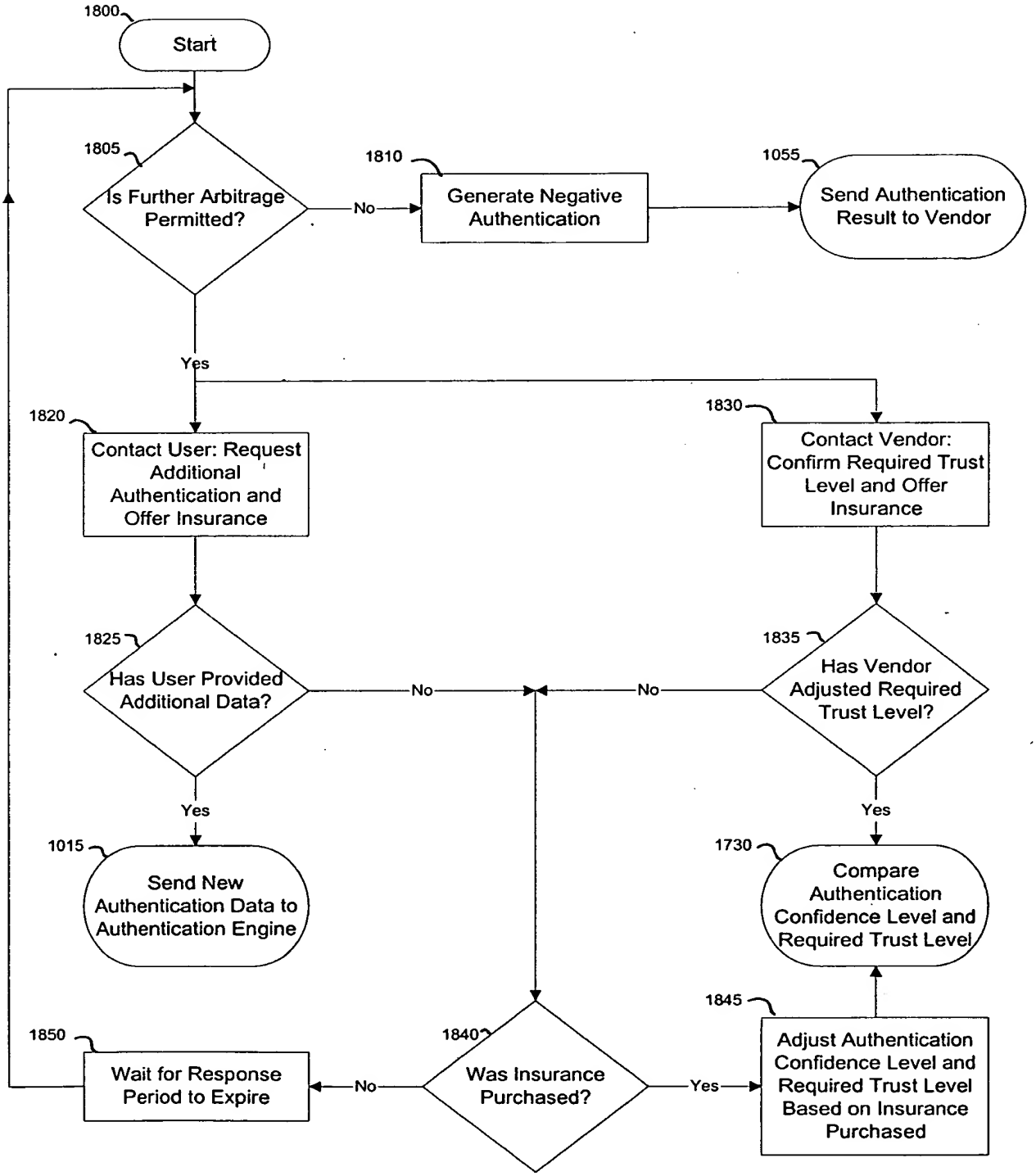

1800
Start
1805
Is Further Arbitrage Permitted?
No
1810
Generate Negative Authentication
1055
Send Authentication Result to Vendor
Yes
1820
Contact User: Request Additional Authentication and Offer Insurance
1830
Contact Vendor: Confirm Required Trust Level and Offer Insurance
1825
Has User Provided Additional Data?
No
No
1835
Has Vendor Adjusted Required Trust Level?
Yes
Yes
1015
Send New Authentication Data to Authentication Engine
1730
Compare Authentication Confidence Level and Required Trust Level
1845
Adjust Authentication Confidence Level and Required Trust Level Based on Insurance Purchased
1840
Was Insurance Purchased?
Yes
No
1850
Wait for Response Period to Expire

FIGURE 19

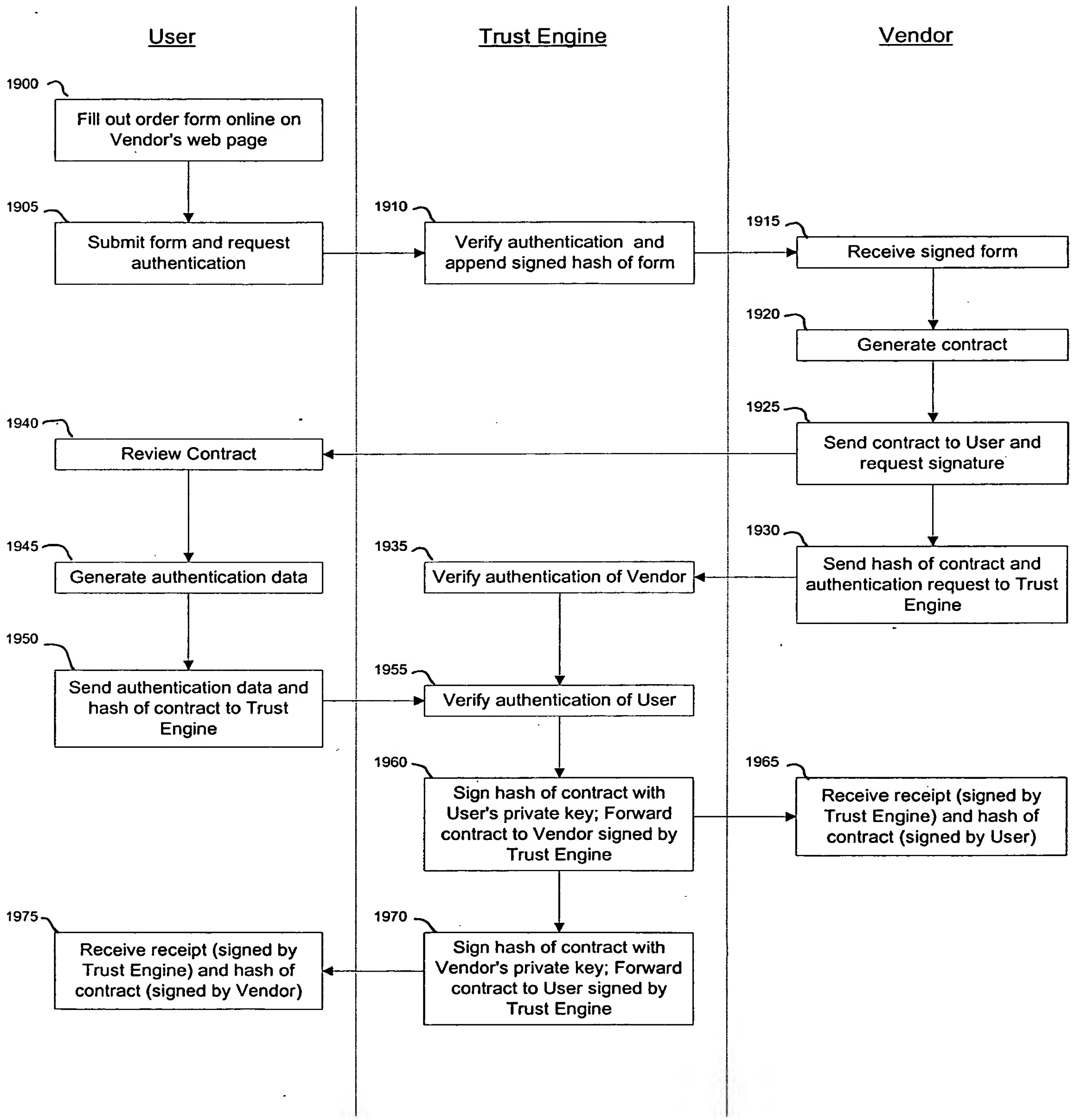


FIGURE 20